Projekte und Vorhaben aus dem Herbst-Treff 2016

- Logging: Inventar von Thomas durchgehen und definieren, was wie lange aufbewahrt werden soll. Doku dazu verfassen und auf UTC hinweisen!
- Alerting: Die Ueberwachung könnte bei gewissen Schwellwerten oder Ausfällen SMS verschicken oder sonst irgendwie intensiver als über Email auf sich aufmerksam machen
- Webstatistik: Kann awstat pro Domain so aufgesetzt werden, dass jeder nur seine Statistik sieht?
- Email-Quarantäne: Können wir Mails, die einen infizierten Anhang haben, so ändern, dass der Anhang durch ein Text ersetzt wird, der sagt, dass der Anhang entfernt wurde?
- Crontab-Files: Backupen mit Snapshot Tool?
- Catch-All: Wie machen wir aus dem Catch-All ein Catch-Rest?
- Wie funktioniert das White-/Blacklisting über LDAP Attribute?
- http://fex.belwue.de/fstools/spamblock Spamblock aktivieren
- Im Spamassassin HowTo könnte man vielleicht ausführen wie man user_prefs geschickt aufpeppt.
- Autoreply: Statt Attribut „mailAutoreply“ in Postfix ein trashnet-eigenes Attribut verwenden. Dies dann im Self-Service implementieren (Auswirkungen auf Phamm?)
- Idee von Chris: Git/Gitlab betreiben
- Idee von Othmar: Bei SCION mitmachen
- Idee von Thomas: PAM- und OpenSSH-Setting –> Time-based One-Time Password
- API-Keys/Web-Service für den Zugriff auf Liste der erlaubten Open DNS Resolver Clients
- Alle eingehenden Mails werden automatisch mit PGP verschlüsselt und in der Mailbox so abgelegt. In Webmail kann man das dann lesen mit https://www.mailvelope.com/de/ Das heißt es wird nichts in Klartext auf der HD abgelegt. Das ganze kann man mit procmail machen aber besser wäre das vorher schon nach der Spam Filterung zu machen (Mehrere Provider bieten das schon an).
- Wie müssen Austritte richtig gemacht werden?
  - Thomas: Das Passwort ändern und bei authorizedServices alle Dienste entfernen. Inaktive Accounts können wir einmal jährlich manuell aufräumen. Der Benutzer kann generell ja irgendwo Dateien liegen haben (auch in /d1, wenn er an einem Projekt mitgearbeitet hat). Wir sollten daher vor dem Löschen vom Account jeweils kurz suchen, ob es vom Benutzer noch Daten ausserhalb des Homeverzeichnisses gibt. Wenn wir den Account gleich löschen, dann verlieren wir das Mapping von UID zu Usernamen.
  - Othmar: Für den Benutzer sollten auch keine Mails mehr angenommen werden, es sollten keine Virtuellen Domains mehr laufen, weder Webdomains noch Maildomains. Auch mailman subscriptions sollten gelöscht werden. Eventuell müssen noch mehr Aspekte beachtet werden.

Gelöste oder entschiedene Themen

- /sw: Prozesse? Was soll da verfügbar sein? Wer entscheidet? ==⇒ Mitglieder melden, wenn sie etwas wollen, Techstaff prüft technisch und wenn gut, implementiert
- UTC oder LocalTime? ==⇒ Nur bei Cron-Jobs und den Logfiles tauchen Zeitstempel in UTC auf. Ansonsten wird dem User immer localtime gezeigt.

- Jabber: Thomas installiert/migriert. Roman bietet an zu testen und eine Anleitung zu schreiben.
- Wiki aufräumen: Folder Plattform-Migration und System Dokumentation → Roman räumt auf

Ideen, die verworfen wurden

- Passive Überwachung ns1/ns2 –> Logging der Dienste und von Shorewall geben genug Info, ein zus. Network-Sniffer bringt da keinen grossen Mehrwert
- Auf msg gewisse Filterungen aktivieren für Posts in die Mailinglisten?
- Bei postgrey wird normaler Syslog genutzt. Man kann in rsyslog Filter definieren. Um ein Beispiel zu geben für einen Eintrag in der rsyslog.conf: – if $programname == 'postgrey' then /var/log/postgrey.log – Da alle Syslogs auf mon1 zusammen laufen, würde ein solcher Filter dort die Logs der beiden postgrey (mail1/mail2) wieder in ein File zusammen mergen. Dann müssten wir dieses Logfile nur noch irgendwie zugreifbar machen.